Ostbayerische Technische Hochschule
Amberg-Weiden

Leitfaden

Passwörter

der OTH Amberg-Weiden

1 Zielsetzung und Definition

Der Zugang zu den IT-Systemen, IT-Diensten und IT-Anwendungen wird über die Zuteilung einer OTH-weiten Benutzerkennung ermöglicht. Dieser Zugang muss über ein Passwort abgesichert werden.

Die vorliegende Richtlinie regelt die Vergabe von Passwörtern an der OTH Amberg-Weiden.
Grundsätzlich erhält jeder Hochschulangehörige bei Aufnahme seiner Tätigkeit an der OTH Amberg-Weiden vom Rechenzentrum seine OTH-weite, individuelle Benutzerkennung mit einem vordefinierten Passwort. Jeder Nutzer ist dann verpflichtet, dieses Standard-Passwort auf ein sicheres, für ihn aber trotzdem leicht zu merkendes Passwort zu ändern.

Der Benutzer ist dafür verantwortlich, dass sein Passwort nur ihm selbst bekannt ist/bleibt und nur er damit Zugang zu den IT-Systemen, IT-Diensten, IT-Anwendungen und anderen eigenen Daten hat.

Diese Richtlinie legt die Regeln bzgl. Passwörter an der OTH Amberg-Weiden fest.

2 Generelle Festlegungen

Das Rechenzentrum der OTH Amberg-Weiden vergibt an jeden Hochschulangehörigen jeweils eine hochschulweite OTH-AW-Benutzerkennung zur Authentisierung/Identifizierung an allen IT-Systemen/Diensten/Anwendungen, d. h. die Benutzerkennung und das zugehörige Passwort ist nur an einer gut gesicherten Stelle gespeichert. Jeder Dienst fragt dort nach, ob das zu der Benutzerkennung eingegebene Passwort korrekt ist. Durch diese OTH-weite Benutzerkennung und dem damit verbundenen Merken nur eines Passworts wird das Arbeiten mit den hochschulweiten IT-Systemen/Diensten/Anwendungen sehr erleichtert. Umso wichtiger ist es deshalb, dass jeder Hochschulangehörige sich umso mehr Gedanken um ein „sicheres“ Passwort (Abschnitt 3) macht und entsprechend sorgfältig mit seiner Benutzerkennung und seinem Passwort umgeht.

Für die Verwendung von Passwörtern an der OTH Amberg-Weiden gelten grundsätzlich folgende Regeln:

- Das Passwort ist ausschließlich dem Hochschulangehörigen bekannt.
- Eine Weitergabe des Passworts an Dritte ist nicht gestattet, auch nicht an eine Vertretung.
- Während der Passworteingabe über Tastatur ist darauf zu achten, dass niemand anderes dabei zusieht.
- Der Zugang wird automatisch für einen gewissen Zeitraum gesperrt, wenn das Passwort mehr als drei Mal falsch eingegeben wurde. Wiederholt sich dies mehrmals, ist hier ein sogenannter Eskalationsmechanismus eingebaut bis es zur endgültigen Sperrung kommt. Bitte nehmen Sie gegebenenfalls telefonischen Kontakt mit Ihrem WGM oder mit dem Rechenzentrum auf.
- Auf keinen Fall dürfen Passwörter per E-Mail mitgeteilt werden!
- Die Passwörter dürfen nur verschlüsselt und auf den minimalsten Zugriff beschränkt auf dem Rechner gespeichert

werden.
- Das Passwort darf nicht aufgeschrieben und beispielsweise unter die Tastatur gelegt oder an den Monitor geklebt werden. Die Verwendung eines Passwortmanager-Tools wie KeePass wird empfohlen.
- Auch darf keine Passwortliste geführt und offen abgelegt werden. Ist das im Einzelfall dennoch notwendig, darf sie nur in einem Safe oder an einem anderen sicheren Ort aufbewahrt werden.
- Das OTH-weit gültige Passwort darf auf keinen Fall auch noch im privaten Bereich bei anderen Anbietern, z. B. bei einem privaten E-Mail-Account, verwendet werden! Ist das der Fall, bitte unbedingt das OTH-Passwort ändern!
- Der Bildschirm kann nach Inaktivität nur mit dem Passwort wieder entsperrt werden.
- Für jeden Dienst ist zwingend ein einzigartiges Passwort zu verwenden. Die Nutzung eines Passworts für mehrere Dienste gleichzeitig ist nicht zulässig.

3 Grundsätze für sichere Passwörter

Eines vorneweg: ein 100% sicheres Passwort gibt es nicht. Ein „sicheres“ Passwort soll vielmehr den Zugang erheblich erschweren. Denn, je mehr Zeit für einen digitalen Einbruch aufgewendet werden muss, desto größer ist die Wahrscheinlichkeit, dass Datendiebe von ihrem Vorhaben abrücken. Ein sicheres Passwort soll also vor allem Zeit schinden. Je komplexer/länger ein Passwort, desto länger benötigen Hacker für dessen Entschlüsselung.

Leicht knackbar ist ein Passwort, wenn:
- es weniger als 8 Zeichen lang ist (Bruteforce-Angriffe, die alle Zeichen-/Ziffern-Kombinationen durchprobieren, sind relativ schnell erfolgreich)
- Sie logische Buchstaben- oder Zahlenreihen verwenden, z. B. asdfghjk oder 12345678
- Sie Wörter verwenden, die in irgendwelchen Wörterbüchern/Lexika hinterlegt sind
- Sie solche „schlechten“ Wörter am Ende mit Ziffern einfach hochzählen
- es sich um ein von vielen Anwendern sehr häufig verwendetes Passwort handelt
- Sie persönliche Informationen, die ein Hacker leicht im Internet über Sie finden kann, verwenden, z. B. Name Ihres Partners, Ihrer Kinder, Ihres Haustieres, usw.

Solche unsicheren Passwörter können Hacker mit minimalem Aufwand in wenigen Sekunden bzw. Minuten leicht knacken.

Um ein möglichst sicheres Passwort zu finden, sollten folgende Grundsätze beherzigt werden:
- Das Passwort sollte mindestens 10 Zeichen lang sein
- Das Passwort sollte sowohl Klein- und Großbuchstaben, Ziffern und Sonderzeichen enthalten
- Keine Verwendung von Name, Vorname, Benutzername
- Keine gängigen Tastaturmuster, keine logischen Zahlen- oder Buchstabenreihen
- Keine Verwendung von Wörtern aus Wörterbüchern/Lexika – auch nicht zusammen mit gängigen Zeichen-Ersetzungsregeln
- Keine Verwendung von leicht herauszufindenden persönlichen Angaben

Je länger das Passwort und je größer der verwendete Zeichensatz, desto sicherer das Passwort, d. h. desto mehr Rechenzeit müsste aufgewendet werden, um ein solches Passwort zu knacken.

Verwenden Sie unter Berücksichtigung der obigen Grundsätze zum Finden eines sicheren Passworts am besten einen ganzen Passwort-SATZ mit einer Länge von mind. 20 Zeichen aus Groß- und Kleinbuchstaben in Kombination mit Ziffern und Sonderzeichen.
An der OTH-AW werden Sie bei der ersten Eingabe Ihres selbst festzulegenden Passworts bereits gezwungen, mindestens 10 Zeichen inkl. Ziffern und Sonderzeichen zu verwenden.

Durch die Verwendung unterschiedlicher Passwörter bei verschiedenen Anwendungen vermeiden Sie, dass, wenn ein Account kompromittiert wird, auch automatisch alle anderen Accounts kompromittiert sind. Sie müssen also nur bei dem einen kompromittierten Account Ihr Passwort ändern.

4 Sicheres Speichern von Passwörtern

Am sichersten wäre es, alle verwendeten Passwörter im Kopf zu haben. Bei der immer größer werdenden Anzahl von Passwörtern, ist das aber oft nicht mehr so leicht möglich.
Um Passwörter sicher aufzubewahren, gibt es mehrere Möglichkeiten:

1. Aufschreiben und Aufbewahrung in einem Tresor
2. Abspeichern im jeweiligen Web-Browser (sicheres Master-Passwort notwendig!)
3. Verwendung eines professionellen Passwortmanager-Tools (sicheres Master-Passwort notwendig!)

5 Passwortmanager-Tool

Grundsätzlich bieten Passwortmanager-Tools die Möglichkeit, für jede Anwendung ein eigenes Passwort zu verwenden und diese sicher, d. h. verschlüsselt, in einem digitalen „Tresor“ zu speichern. Der Zugriff darauf ist über ein einziges Master-Passwort abgesichert.

Als Passwortmanager-Tool ist aktuell KeePass zu empfehlen. Sie finden den Download-Link auf unserer Homepage unter https://www.oth-aw.de/informieren-und-entdecken/einrichtungen/rechenzentrum/downloads/#dateien. Das zugehörige deutsche Sprachpaket benötigen Sie ebenfalls für die Installation.

KeePass ist eine Single-User-Anwendung, d.h. jeder Benutzer darf nur seine eigenen KeePass-Datenbank verwalten. Es ist nicht erlaubt, eine KeePass-Datenbank für eine ganze Abteilung/Fakultät anzulegen, die dann von mehreren Personen genutzt werden soll. Dadurch würden mehrere Personen für dieselbe Anwendung denselben Benutzernamen und dasselbe Passwort benutzen.

KeePass erzeugt eine verschlüsselte Datenbank zur Verwaltung von Passwörtern. Abzusichern ist die Datenbank über ein starkes Master-Kennwort, das man sich als einziges merken muss.
Für die einzelnen mit Passwort abzusichernden Anwendungen steht ein Kennwortgenerator zur Verfügung, der automatisch Passwörter beliebiger Länge und Typs generiert, so dass man sich nicht jedes Mal selbst ein Passwort ausdenken muss.
Um bei der jeweiligen Anwendung das geforderte Passwort einzugeben, gibt es mehrere Möglichkeiten:

- Kopieren des Benutzernamens und des Passworts aus KeePass in die Zwischenablage und Einfügen in die Anwendungsanmeldung
- Auto-Type: Automatisches Einfügen über KeePass mit dem globalen Tastenkürzel „Strg+Alt+a“
- Browser-Erweiterungen mit KeePass-Plug-in (ab Version 2.x)

Mittels KeePass ist es ein Leichtes, für jede Anwendung ein eigenes Passwort zu verwenden und sicher zu verwalten.
Sichern Sie bitte Ihre KeePass-Datenbank (Dateiextension .kdbx) unbedingt regelmäßig, z. B. auf H:\.

6 Passwortänderung

Je länger (über die Zeit) und öfter ein vielleicht auch noch schwaches Passwort verwendet wird, desto höher ist die Chance, dass es geknackt oder bekannt wird.

Lange Zeit war deshalb die Empfehlung vom Bundesamt für Sicherheit in der Informationstechnik (BSI), Passwörter regelmäßig zu ändern. Gemäß dieser Empfehlung wurde an der OTH Amberg-Weiden bisher jeder Benutzer nach 180 Tagen gezwungen, sein Passwort zu ändern.
Seit Anfang 2020 empfiehlt das BSI keine erzwungene regelmäßige Passwortänderung mehr mit der Begründung, dass dies eher zu immer schwächeren Passwörtern führe. Das BSI empfiehlt jetzt, Passwörter nur mehr zu ändern, wenn es in fremde Hände geraten sein könnte. Umso wichtiger ist die Vergabe eines möglichst sicheren Passworts (vgl. Abschnitt 3). Das Rechenzentrum der OTH Amberg-Weiden erzwingt derzeit keine halbjährliche Passwortänderung

mehr, sondern nur mehr eine jährliche Änderung.
Das OTH-weit gültige Passwort ist auf jeden Fall zu ändern, falls der Benutzer es auch privat im Internet und bei anderen Anbietern verwendet (hat) oder das Passwort offensichtlich bekannt wurde.

Einen Link zur Änderung des Passwortes des OTH-Accounts ist unter https://sspr.oth-aw.de zu finden. Dabei ist das alte Passwort und zweimal das neue Passwort einzugeben. Beachten Sie dabei die Grundsätze für sichere Passwörter (vgl. Abschnitt 3).
Dieses neue Passwort muss auf allen mobilen Geräten (Laptops, Smartphones, Tablets), bei denen eine Datensynchronisation über https://www.oth-aw.de/informieren-und-entdecken/einrichtungen/rechenzentrum/services/#smartphone-synchronisation stattfindet, geändert werden.
Bei Verwendung von Eduroam ist das bestehende Profil zu löschen und im Anschluss daran das Konfigurationstool auf den betroffenen Geräten über die Webseite https://cat.eduroam.de zu starten. Das Konfigurationstool leitet Schritt für Schritt durch die Konfiguration und fordert auf, das soeben neu vergebene Passwort einzugeben.

7 Überprüfung Ihrer E-Mail-Adresse

Auf folgender Webseite können Sie überprüfen, ob Ihre OTH-E-Mail-Adresse und gegebenenfalls das zugehörige Passwort schon einmal bei einem Cyberangriff aufgetreten ist:
https://sec.hpi.de/ilc/search?lang=de.

8 Zwei-Faktor-Authentifizierung (2FA)

Da Passwörter nie 100% sicher sind, wird zur weiteren Absicherung oft noch ein zweiter Faktor, z. B. eine an eine hinterlegte Handynummer geschickte Codenummer, die der Anwender zusätzlich bei der Anmeldung eingeben muss, herangezogen. Hier spricht man von einer 2-Faktor-Authentifizierung.
Dem Hacker reicht dann nicht das Knacken des Passworts, sondern zusätzlich müsste er auch an das Handy des Anwenders herankommen.
Eine 2FA macht es nahezu unmöglich, einen Anmeldevorgang zu knacken.
Zum Einsatz kommt eine 2FA bereits beim Online-Banking oder bei bestimmten Softwareprodukten, die mit sehr sensiblen Daten arbeiten, z. B. VIVA.
Zukünftig wird es sicher immer mehr Zwei-Faktor-Authentifizierungen geben.

Dokumenteninformationen

Klassifikation:	V1 (öffentlich)
Titel:	Leitfaden Passwörter
Versionsnummer:	1.1
Stand vom:	10.03.2021
Compliance-Bezug:	Gesetzlich: - Vertraglich: - Richtlinien: -
Dokumentenverantwortlicher:	Barbara Kostial (ISB)
Freigabedatum:	01.04.2021
Freigabe durch:	Rechenzentrum, CIO
Mitgeltende Dokumente:	-
Revisionsintervall:	jährlich
Letzte Revision:	-

Dokumentenverteiler

Verteilerkreis (Berechtigte Rolle):	jeder

Dokumentenhistorie

Datum	Bearbeiter	Version	Bemerkung/Änderung
01.07.2020	Barbara Kostial (ISB)	1.0	Erstellung
18.01.2021	Barbara Kostial (ISB)	1.1	Einarbeitung der Korrekturen von A. Aßmuth (CIO)
10.03.2021	Barbara Kostial (ISB)	1.1	Einarbeitung der Korrekturen von A. Aßmuth (CIO)